TERMS, PROCEDURE AND MODE

FOR THE USE OF
QUALIFIED ELECTRONIC SIGNATURE
AND
TIME STAMP TOKEN

Version 1.0

February, 2012

CONTENTS

LIST OF TERMS AND ABBREVIATIONS 3

INTRODUCTION 4

I. TERMS, PROCEDURE AND MODE FOR THE USE OF QUALIFIED ELECTRONIC SIGNATURE 5

1. General rules on the use of the signature 5
2. Rules for signing ..... **Error! Bookmark not defined.**
3. Way of use – trusted software applications 6
4. Constrains on the use of the signature 6
5. Obligations of the Author and the Titular upon signing 7
6. Technical security and control 7
7. Secrecy of the private key 7
8. Generation of a new pair of keys 7
9. Compromising of the private key 8
10. Destroying of private key 8
11. Activation and deactivation of private key 8

II. ACCEPTANCE OF THE SIGNATURE 8

1. Confidence in the electronic signature 8
2. Due care of the Trusting party 8

III. TERMS, PROCEDURE AND MODE OF USE OF THE TIME STAMP TOKEN 11

1. General rules 11
2. Issue of TST 11
3. Mode of use of TST 11
4. Constrain of the use of TST 11
5. Obligations of the parties in the use of TST 11
6. Technical security and control 12

IV. ACCEPTANCE OF THE TIME STAMP TOKEN 12

1. Confidence in the TST 12
2. Due care of the Trusting party 12

List of terms and abbreviations

In English language:

B-Trust®	Търговска марка на дейността на „Борика-Банксервиз" АД като ДУУ / Trade mark of the activity of "Borica - Bankservice" JSC as CSP
CA	Certificate Authority – Удостоверяващ орган
CRL	Certificates Revocation List – Списък на прекратени удостоверения
ETSI	European Telecommunications Standard Institute – Европейски институт за телекомуникационни стандарти
FIPS	Federal Information Processing Standard – Федерален Стандарт за обработка на информация
ISO	International Standard Organization – Международна Организация по стандарти
OID	Object Identifier – Идентификатор на обект
OCSP	On-line Certificate Status Protocol – Протокол за проверка на статус на удостоверение в реално време
PKCS	Public Key Cryptography Standards – Криптографски Стандарти на публични ключове
PKI	Public Key Infrastructure – Инфраструктура на публични ключове
RA	Registry Authority – Регистриращ орган
RSA	Rivers-Shamir-Adelman – Криптографски алгоритъм (асиметричен)
SSCD	Secure Signature Creation Device –Устройство за създаване на сигурен електронен подпис
SHA	Secure Hash Algorithm – Хеш функция
SSL	Secure Socket Layer – Защитена HTTP сесия
TSA	Time Stamp Authority – Орган на удостоверения за време
TST	Time Stamp Token – Удостоверение за време

In Bulgarian language:

АД/JSC	Акционерно дружество /Joint-Stock Company
ДУУ/CSP	Доставчик на Удостоверителни Услуги/Certificate Services Provider
ЗЕДЕП/LEDES	Закон за електронния документ и електронния подпис/Law on Electronic Document and Electronic Signature
ЗЕУ/LEG	Закон за Електронно Управление (е-Управление)/Law on Electronic Governance (e-Governance)
КРС/CRC	Комисия за регулиране на съобщенията/Communications Regulation Commission
МРС/LRO	Местна Регистрираща Служба/Local Registry Office
НДДУУ/OACSP	Наредба за дейността на доставчиците на удостоверителни услуги/Ordinance on the Activities of Certificate Service Providers
НИАКЕП/ORQESA	Наредба за изискванията към алгоритмите за квалифициран електронен подпис/Ordinance on the Requirements for Qualified Electronic Signature Algorithms
Наръчник/User Manual	Наръчник на потребителя за предоставяните от "БОРИКА - БАНКСЕРВИЗ" АД B-TRUST® удостоверителни, информационни, криптографски и консултантски услуги за квалифициран

	електронен подпис/User Manual on the provision of certification, information, encryption and consulting services for qualified electronic signature by "BORICA - BANKSERVICE" JSC B-TRUST ®
Практика/CPS	Практика на предоставяне на удостоверения за квалифициран електронен подпис, Практика на органа за удостоверяване на време/ Certificate Practice Statement of the QES Certificate Services Provider, Certificate Practice Statement of the Time Stamp Authority
Политика/CP	Политика на предоставяне на удостоверения за квалифициран електронен подпис, Политика на органа за удостоверяване на време/ Certificate Policy of the QES Certificate Services Provider, Certificate Policy of the Time Stamp Authority
КЕП/QES	Квалифициран Електронен Подпис/Qualified Electronic Signature

Introduction

This document describes:

- The mode of use of the qualified electronic signature (QES), for which the relevant qualified certificate has been issued on the Author/Titleholder, as well as the mode of use of the time stamps token issued by the CSP "BORICA-BANKSERVICE" JSC;
- The terms and procedure for the use of QES, including the requirements for the treasure up of the Author's/Titular's private key, and the terms and procedure for the use of the time stamps token;
- Terms for the access to a certificate for QES and time stamp token, as well as the method to verify the QES and the time stamp token.

Based on this document each Author/Titular of certificates for QES and/or Trusting party of a QES and of a TST shall be able to define, to create and to follow a concrete Policy on signing/verifying of QES, as well as a Policy on the use of TST.

I. TERMS, PROCEDURE AND MODE FOR THE USE OF QUALIFIED ELECTRONIC SIGNATURE

1. General rules on the use of the signature

1.1. Each Author/Titular utilizes QES in abiding by the following basic requirements:

- In adhering strictly to LEDES, to the ordnances on the law implementation and on the commonly established in the CPS recommendations and standards;
- In observing the highest level of treasure up/protection of the private key for electronic signature by the Author/Titular;
- In adhering to the terms and procedures for generating the pair of keys in accordance with the User Manual, regardless of whether the above-mentioned pair of keys shall be generated by the CSP or by the Author/Titular;
- In observing the terms for access to the private key – use of password/personal identification number (PIN);
- In strict compliance with the measures and procedures for identification and authentication of the applicant party for a qualified certificate for QES, according to the User Manual;
- In the impossibility for a subsequent use of QES after a smart-card loss, after destruction of the private key for signing, after expired validity or termination of an adequate certificate;
- In publicly announced CPS, procedures and CP for the provision of certificate services by the CSP;
- In 24/7 public access to the Public Register for the issued CRL for QES and to the service certificates of the CSP through its Internet site;
- In observance of the guarantees and the insurance policy of the CSP;
- In respecting of the moral and property rights, in particular the intellectual property rights of the CSP and the Author/Titular.

2. Rules for signing

2.1. Before using the private key for signing an electronic document the Author/Titular must be sure that the corresponding certificate is for QES, i.e. the certificate is qualified and it is issued in accordance with the CP for this certificate, and the CP meets the Author/Titular needs;

2.2. It is recommended to check the CP by comparing with the identifiers, specified in the original copy of the User Manual of the CSP;

2.3. The CP on issuance and maintenance of the certificate for QES is identified in the same certificate with the following characteristics:

- Unique CP OID;
- Unique identifier for qualified certificate;
- Name of the CSP;
- Date of issue and date of entry into force of the CP, which is a consequence of the date of issue and the date of entry into force of the User Manual;
- Applicability to the specific type of certificate.

3. Way of use – trusted software applications

3.1. Signing with QES must always be performed with trusted software applications or with software applications certified by the LEG.

3.2. On the CSP's website there is a published list with the trusted software applications suitable for the use of QES and for the relevant certificate, in accordance with its purpose;

3.3. It is in the due care of the Trusting party to check the purpose and the applicability of the certificate for QES and the software applications used for the creation and verification of the signature.

3.4. The signing party, respectively the Trusting/verification party principally implements two ways for signing with QES and for verifying the signature:

- Local – the trusted software application for signing/verification will be operational for the local at the Author/Titular system, as for signing, the local reader with the smart-card containing the QES will be available. This way of operation refers to the use of the widely spread and de-facto established as standards software applications for e-documents (MS Office, Adobe Acrobat, etc.) or for clients' software packages and instruments for signing/verification provisioned by the CSP;
- Remote – the trusted software application for signing/verification operates as a service in the server system, as for signing, a remote access to the reader with the smart-card containing the QES for the local system is available to the Author/Titular. CSP provides online services for signing/verification.

4. Constrains on the use of the signature

4.1. QES has legal value of a handwritten signature, if used with an accompanying qualified certificate for QES, within the scope of this certificate, as well as, in terms of additionally agreed between the Author/Titular and the Trusting party constrains on the way of use.

4.2. Constrains on the use of the signature in terms of value of the transactions, which the Author/Titular may conduct with QES and the statements that may be delivered by the Author/Titular, are outside of the scope of the CP, under whose CP the CA of the CSP provisions the relevant certificate for QES. The restriction on the use of the issued certificates in respect to the value of the transactions, which the Author/Titular may conduct with QES, is subject to concordance between the Author/Titular and the Trusting party.

4.3. Constrains on the use of QES in terms of its purpose shall be recorded in the certificate by the requisites “Key Usage” and “Extended Key Usage”.

4.4. The use of QES outside the recorded in the certificate constrains shall not engage in any way the responsibility of the CSP and is borne entirely by the Author/Titular or by the Trusting party. In this case, the QES, accompanied by such a certificate loses its legal value of such qualified signature.

5. Obligations of the Author and the Titular upon signing

5.1. Upon use of QES the Author/Titular must:

- Follow and comply strictly with the terms and procedures in the User Manual, and the corresponding policies and practices for the use of the signature and the consumption of other certification services;
- Have a basic knowledge on the use of electronic signature and PKI technologies;
- Not use the private key to create QES after the expiry of the certificate, or after suspension or termination of the certificate’s validity;
- Notify each Trusting party on the due care taken in trusting QES and its accompanying qualified certificate.

6. Technical security and control

6.1. Detailed information on the requirements for treasure up the private key and on the creation of QES of an Author/Titular is contained in the User Manual of the CSP.

7. Secrecy of the private key

7.1. In order to protect the secrecy of the private key the Author/Titular must:

- Ensure secure and trusted environment when using the pair of keys for the QES with a view to protect the secrecy of the private key;
- Use algorithms, according to the requirement of ORQESA;
- Notify immediately the CSP in case of compromising or having suspicions for compromising the private key, by requesting simultaneous suspension or termination of the relevant certificate for the QES;
- Treasure up and protect reliably against loss and compromise the secrecy of its private key for the validity period of the certificate, according to the requirements set up in the User Manual of the CSP. Each use of the private key shall be considered as an action committed by the Author/Titular;
- Change the initially provisioned PIN-code for access the smart-card (private key) before using the QES, in case that the qualified certificate has been issued on a B-Trust smart-card.

8. Generation of new pair of keys

8.1. In view of reducing the risk from compromising the current pair of keys, the CSP recommends that the Author/Titular generates new pair of keys when renewing or reissuing certificate for QES.

9. Compromising of the private key

9.1. According to the User Manual of the CSP, in case of compromising the Author's/Titular's private key, the latter shall immediately notify the CSP for initiating a procedure on termination the certificate.

10. Destroying of a private key

10.1. An Author/Titular destroys the private key by using:

- Iinitialization ("deletion") of the smart-card if the key is treasured up on a smart-card;
- Physical destruction of the media (smart-card).

11. Activation and deactivation of private key

11.1. Upon initialization of B-Trust smart-card the following access codes shall be generated, and shall be provisioned to the Author/Titular: code to unblock the card "Unblock PIN" and initial user access code „User PIN".

11.2. The Author/Titular is obliged to change the „User PIN", through the software provisioned with the B-Trust smart-card.

11.3. The CSP recommends that, the Author/Titular shall change periodically the user access to the smart-card code „User PIN".

11.4. The Author/Titular shall duly treasure up and shall use only when necessary the provisioned code to unblock the smart-card "Unblock PIN".

11.5. The access to the private key for creating QES shall be implemented by inserting the smart-card into the card reader and entering the „User PIN"or carrying out personal identification in any other way.

11.6. A private key for creating QES shall be deactivated by termination of the certificate for this QES.

11.7. If the private key has been saved on a smart-card, the possibility of using it shall be terminated by removing the smart card from the card reader.

11.8. If the private key has been saved on other media, the possibility of using it shall be terminated by removing the media from the computer and suspending the access to the key file.

II. ACCEPTANCE OF THE SIGNATURE

1. Confidence in the electronic signature

1.1. The Trusting party - the addressee of an electronic statement or signed with QES electronic document of the Author/Titular shall accept and trust, that the signature has legal value of a handwritten signature to the Trusting party and binds the Author/Titular only after due care is taken to check all circumstances concerning the validity of the applied electronic signature.

2. Due care of the Trusting party

2.1. The use of QES implies that persons who trust the qualified certificate for the signature shall have basic knowledge on the principles of operation of the B-Trust PKI Infrastructure of CSP.

2.2. The Trusting party shall take due care as:

- Trusts the certificate only in view of the purpose and terms of the CP, according to which the certificate has been issued and takes into account the additionally agreed and contracted with the Author/Titular constrains for using the QES in Trusting party relations with the Author/Titular;
- Checks the certificate for the indicated CP applicable to this certificate ("Certificate Policy") and the purpose and constraints on the certificate validity;
- Checks the purpose of the signature through the fields: "Key Usage", "Extended Key Usage" and "Qualified Statement" in the certificate. The field "Basic constrains" must be established as follows: “Subject Type = None”. The field "Key Usage" must contain "Non-repudiation, Digital Signature". The field "Qualified Statements" must contain the identifier ‘0.4.01862.1’;
- Checks constrain, on the use of the certificate with respect to the value of the property interest, if any. In the general case, constrain is beyond the scope of the CP of the CSP for a qualified certificate for QES and is subject to concordance and agreement between the Author/Titular and the Trusting party. The constrain, if any, shall not refer to Provider’s responsibility for damages of the issued certificate for QES;
- Determine whether the certificate is issued for test demonstration needs.

2.3. The Trusting party shall ensure that the issued certificate is for QES. The verification shall be performed:

- On the basis of the recorded OID for the CP under which the certificate has been issued by the CSP;
- Based on the content in the field "Qualified Statements";
- Based on the content in the field "Subject", through the string "Personal Certificate - UES", respectively "Professional Certificate - UES", if this string presents.

2.4. The Trusting party must check the format of the data that have been signed - to verify the electronic signature, it is necessary to know exactly what information or object were signed. The established international recommendations, standards and specifications for public key cryptography set the standard formats for QES application to an electronic statement or document of the Author/Titular: PKCS # 7, CMS, XML-DSIG, XAdES, etc.

2.5. The Trusting party must verify that the CSP is registered in the published Register of the CSP under LEDES requirements.

2.6. The Trusting party must ensure that the Author is the person recorded in the certificate and acts within his/her power of attorney in respect to the Titular, if such registered.

2.7. The Trusting party must verify the status of the qualified certificate in the supported by the CSP Public Register. The verification of the authenticity and integrity of the certificate – i.e. signature of the CSP does not provide verification of its validity and all the damages occurred from the actions undertaken after completion of such verification shall be borne by the Trusting party.

2.8. The Trusting party must verify by checking to an acceptable level of confidence such as: operational certificate of the CSP, whether the certificate of the Author/Titular has not been terminated or suspended. The termination or suspension of the certificate as a legal consequence leads to the invalidity of the signature. Validation status shall be carried out by using CRL, OCSP or review the Register for certificates of the CSP.

2.9. The Trusting party must check/verify the digital signature for the electronically signed statements, and verify the electronic signature of the CSP through the chain of certificates up to an acceptable level or to the root certificate. This verification is based on the X.509 standard. The validation of the QES shall be in respect to the successful confirmation of the validity of the certificates in throughout the whole chain in which the certificate for QES participates. Particularly for the domain B-Trust, in this chain are involved the root certificate of the CA "B-Trust Root CA" and the operational certificate of the CA "B-Trust Operational CA QES".

2.10. The Trusting party shall ensure that the applications with which the certificate is in use are functionally applicable for the purpose the certificate was issued, as well as in view to the security levels specified in the respective CP.

2.11. The Trusting party shall ensure that such acceptance is reasonable under relevant circumstances. In the event that the circumstances require the need for additional safeguards for trust and confidence, the Trusting party must offer an adequate proper care for building full trust and confidence.

2.12. It is in the Trusting party due care taken to use a mechanism for a secure signature verification, which ensures that:

- The public key, which is used for the actual check of the signature corresponds to what is displayed on the screen;
- The verification of using the private key is reliably confirmed and the verification results are displayed correctly;
- The Trusting party may, if necessary determine the contents of the signed electronic document;
- The authenticity and validity of the certificate at the time of signing/use of QES are reliably tested;
- The results from the verification and the electronic identity of the Author/Titular are properly visualized;
- Any changes relevant to the security are identifiable.

2.13. CSP shall not be responsible for any damages to the Trusting party derived from failure to take a due care.

III. TERMS, PROCEDURE AND MODE OF USE OF THE TIME STAMP TOKEN

1. General rules

1.1. The CP of the specialized authority of the CSP for TST contains the terms and procedures for the issuance, supply and maintenance of TST for the users.

1.2. CSP issues TST to any interested party by respecting a standard/unguaranteed level of service.

1.3. User who needs a guaranteed level of service of the TST concludes a contract with CSP.

1.4. CSP issues TST with two types of content – for QES and for any electronic document.

1.5. The TST must be published in the Public Register for TST to the specialized TSA of CSP.

2. Issue of TST

2.1. The CSP issues TST under the common CP with an identifier „OID = 0.4.0.2023.1.1".

2.2. TSTs with CP identifier different from the above-shown shall be issued to users, who have a contract with the CSP for Service Level Agreement (SLA) for the TST.

3. Mode of use of TST

3.1. TST with Policy identifier „OID = 0.4.0.2023.1.1" are applicable for use in applications with different profile:

- Use of the QES to a specific point in time – TST is integrated to the QES of the signed document. This use of TST creates "non-repudiation" of QES over the time - i.e. the validity of QES extends beyond the period of validity of the qualified certificate for this QES. This mode of use of TST enables to utilize extended format of QES (XAdES, CAdES, PAdES) in the corresponding applications;
- Creating a certificate with content of an electronic document before a certain point in time, i.e. a certificate with irreversible content of the electronic document after the moment of the TST. This mode of use of TST is applied in building of archives, registers, e-forms, etc.

3.2. TST with coordinated CP of issuance and use shall be administered in specialized applications for the TST users.

4. Constrain on the use of TST

4.1. TSTs with common CP identifier „OID = 0.4.0.2023.1.1" in the TST itself shall not constrain the applicability of the provided TST, at the discretion of the users.

4.2. TSTs with coordinated CP of issuance and use, included in these TSTs shall only serve specific parties, under the terms of the contract with the CSP. CSP shall not be responsible when the applicability of the TST is beyond the CP indicated in the TST.

5. Obligations of the parties in the use of TST

5.1. The obligations and responsibilities of CSP for the provision and maintenance of TST with common CP identifier "OID = 0.4.0.2023.1.1" are described in the document

"Certificate Policy and Certificate Practice Statement of the Authentication B-Trust Time Stamp Authority" of the CSP.

5.2. The obligations and responsibilities of CSP for the provision and maintenance of TST with coordinated CP identifier shall be described in separate document Service Level Agreement (SLA), which is integral part of the contract with the CSP.

5.3. The TST users must:

- Accept the root certificate of the CSP, thus building the confidence to this CSP and its specialized TSA;
- Use the qualified certificate of the TSA for the purpose to verify the QES in the TST;
- Carry out verifications of QES by following the instructions in this document.

5.4. The Trusting party must verify QES in the TST and the validity of the certificate of the TSA.

5.5. In the event that the certificate has expired the Trusting party must:

- Check in CRL for this certificate;
- Verify the security level of the used Secure Hash Algorithm according to the CP;
- Check the security level of the algorithms and the length of the key pair of QES.

6. Technical security and control

6.1. The technical security and control with the use of TST are in full compliance with the public document "Certificate Policy and Certificate Practice Statement of the Authentication B-Trust Time Stamp Authority" of the CSP.

IV. ACCEPTANCE OF THE TIME STAMP TOKEN

1. Confidence in the TST

1.1. The Trusting party - addressee in the use of TST must trust and accept, that TST has official certification power to it and binds the CSP, only after due care is taken to verify all the circumstances concerning their validity of the issued TST.

2. Due care of the Trusting party

2.1. The Trusting party must check in the CSP's Public Register for a TST with this concrete number.

2.2. Must take due care by following the instructions mentioned and described in this document.